Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Plains Midstream Canada ULC (Organization)
Decision number (file number)	P2022-ND-007 (File #022142)
Date notice received by OIPC	July 8, 2021
Date Organization last provided information	July 8, 2021
Date of decision	May 5, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • first and last name, • date of birth, • home address, • phone number, • email address, • employer, • department, • date of hire, • average number of hours worked per week, • last day worked prior to starting leave, • number of remaining sick days, • confirmation that a disability claim has been filed and whether the claim is WCB, short term or long term disability, • confirmation of whether such disability claim has been approved, pending or rejected, • manager's first and last name, and work phone number, • human resource partner's first and last name, and work phone number, and • potential notes from the affected individual's doctor.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third party service provider (Dynamic Insight Corp. or "Dynamic") that assists the Organization with short term disability claim management. • Dynamic receives the Organization's employee claim information in order to assist with the provision of this service. • On June 22, 2021, Dynamic notified the Organization that a Dynamic's employee email account was accessed by an unauthorized individual on or about March 1, 2021. • Dynamic was unable to determine the cause of the unauthorized access.
Affected individuals	The incident affected two (2) individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	<u>Dynamic:</u> • Investigated the incident. • Acted on information and changed all passwords. • Offered credit monitoring and identify theft protection. <u>Organization:</u> • Requested Dynamic to remove personal, health information and other sensitive information from Exchange online and store such information on a secure server or print and file. • Requested Dynamic password protect/encrypt personal, health information and other sensitive information, change passwords every 90 days, perform penetration testing and evaluate their security program each year. • Reported to the Privacy Commissioner of Canada.

Steps taken to notify individuals of the incident	Affected individuals were notified by letter via email on July 8, 2021.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported, *It was determined that a real risk of significant harm exists, given the highly sensitive nature of the potential personal information that may have been impacted, which could allow for identity theft or potentially impact the credit record of the affected employee. Further, it was determined that the information disclosed is highly sensitive because it discloses health information, and that an individual is seeking or is currently on leave for medical reasons, which could result in loss of professional opportunities, damage to reputation, humiliation and other negative effects.* I agree with the Organization's assessment. A reasonable person would consider that contact and identity information could be used to cause the significant harms of identity theft and fraud. Email addresses, particularly in conjunction with employment information, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The disability and medical information could be used to cause hurt, humiliation, and embarrassment, as well as damage to reputation and/or loss of professional opportunities. These are all significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported, *Plains has no knowledge that any personal information was misused. Given the highly sensitive nature of personal information as provided in s.11, there is a real risk of significant harm in the event such information is misused.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (unauthorized access). Although the Organization reported it has "no knowledge that any personal information was misused", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft, fraud and the other harms listed above can happen months and even years after a data breach. Further, it appears the email account was exposed for approximately ten (10) days.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals. A reasonable person would consider that contact and identity information could be used to cause the significant harms of identity theft and fraud. Email addresses, particularly in conjunction with employment information, could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. The disability and medical information could be used to cause hurt, humiliation, and embarrassment, as well as damage to reputation and/or loss of professional opportunities. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (unauthorized access). Although the Organization reported it has "no knowledge that any personal information was misused", I do not believe that the lack of reported incidents of identity theft or fraud to date is a mitigating factor in the likelihood of harm resulting from this incident. Identity theft, fraud and the other harms listed above can happen months and even years after a data breach. Further, it appears the email account was exposed for approximately ten (10) days. I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter via email on July 8, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance